ON THE CONJUGACY PROBLEM FOR F/R'

C. K. GUPTA¹

ABSTRACT. Let F/R be a finitely generated recursively presented group with the solvable conjugacy problem and the solvable power problem. The conjugacy problem for F/R' when F/R is torsion free has been solved by Remeslennikov and Sokolov (Algebra and Logic 9 (1970), 342–349). In this note we prove that F/R' has the solvable conjugacy problem even when F/R is not torsion free. This allows us, in particular, to conclude the solvability of the conjugacy problem for $F/[F^n, F^n]$ in terms of the conjugacy problem for F/F^n .

Summary. If the conjugacy problem and the power problem for F/R is solvable, then the conjugacy problem for F/R' is solvable.

Introduction. Let F/R be a finitely generated recursively presented group with the solvable conjugacy problem and the solvable power problem. The conjugacy problem for F/R' when F/R is torsion free has been solved by Remeslennikov and Sokolov [6]. In this note we are able to prove that F/R' has the solvable conjugacy problem even when F/R is not torsion free. This allows us, in particular, to conclude the solvability of the conjugacy problem for $F/[F^n, F^n]$ in terms of the conjugacy problem for F/F^n . As in [6] our tool is the Magnus embedding of F/R' into a group of 2×2 matrices and a result of Matthews [5] about the conjugacy problem for the restricted wreath product of two groups.

Preliminary results. Let F be a noncyclic free group on a finite set X and R a normal subgroup of F . Let Ω be the free left $Z(F/R)$ -module with basis $\{\lambda_x | x \in X\}$. Then every element of Ω is of the form

$$f = \sum_{x \in X} f_x \lambda_x, \quad f_x \in Z(F/R).$$

For $w \in F$, we set $Rw = \mathbf{w}$ and consider the group

$$M = \begin{pmatrix} F/R & \Omega \\ 0 & R/R \end{pmatrix}$$

of 2×2 matrices of the form

$$\begin{pmatrix} \mathbf{w} & f \\ 0 & 1 \end{pmatrix},$$

$w \in F$, $f \in \Omega$. It is easily verified that M is isomorphic to the restricted wreath product of a free abelian group of rank $|X|$ by F/R . Thus, by a result of Matthews [5], we have

Received by the editors October 6, 1980.

1980 *Mathematics Subject Classification*. Primary 20F10.

¹Research supported by the Natural Sciences and Engineering Research Council Canada.

LEMMA 1. *If F/R has the solvable conjugacy problem and the solvable power problem² then M has the solvable conjugacy problem.*

Let $\varphi: F \rightarrow M$ be the homomorphism defined by

$$\varphi(x) = \begin{pmatrix} \mathbf{x} & \lambda_x \\ 0 & 1 \end{pmatrix}, \quad x \in X.$$

Then a well-known result of Magnus [4] states that the kernel of φ is R' . Thus F/R' is embedded in M and we shall identify the elements of F/R' in M by

$$\varphi(w) = \begin{pmatrix} \mathbf{w} & \alpha(w) \\ 0 & 1 \end{pmatrix}.$$

The matrix multiplication yields the following lemma (see, for instance, [2, Lemma 2.1]).

LEMMA 2. *Let $\alpha(w)$ be the 12-entry of $\varphi(w)$. Then*

- (i) $\alpha(uv) = \mathbf{u}\alpha(v) + \alpha(u)$ for $u, v \in F$;
- (ii) $\alpha(w^{-1}rw) = \mathbf{w}^{-1}\alpha(r)$ for $w \in F, r \in R$;
- (iii) $\alpha(w^{-1}) = -\mathbf{w}^{-1}\alpha(w)$;
- (iv) $\alpha(x) = \lambda_x$;
- (v) $\alpha(1) = 0$.

The next lemma gives a criteria for an arbitrary element $f \in \Omega$ to be $\alpha(r)$ for some $r \in R$.

LEMMA 3 (REMESLENNIKOV AND SOKOLOV [6]). *Let $f = \sum_x f_x \lambda_x \in \Omega$. Then $f = \alpha(r)$ for some $r \in R$ if and only if $\sum_x f_x (\mathbf{x} - 1) = 0$ in $Z(F/R)$. [Since*

$$\begin{pmatrix} \mathbf{a} & f \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & f - \alpha(a) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathbf{a} & \alpha(a) \\ 0 & 1 \end{pmatrix},$$

Lemma 3 can be used to determine if $f = \alpha(ra)$ for some $a \in F, r \in R$.]

Finally, we shall need the following lemma about finitely generated groups with the solvable word problem.

LEMMA 4. *Let G be a finitely generated group with the solvable word problem. Let a be an element of G of finite order $n \geq 2$. If $(a - 1)u = 0$ for some $u \in \mathbb{Z}G$, then $u = p(a)v$, where $p(a) = 1 + a + \dots + a^{n-1}$ and $v \in \mathbb{Z}G$ can be effectively determined.*

PROOF. Let $A = \text{sgp}\{a\}$ and let $S = \text{supp}_G(u)$ be the support of u . Let $S = \bigcup_{i=1}^l S_i$ be the partition of S determined by the property: $g, h \in S_i$ if and only if $Ag = Ah$ (this can be tested using the word problem for G). We choose a representative σ_i for each S_i . Then $g \in S$ implies $g = k^{(i)}\sigma_i$ for some $k^{(i)} \in \{0, \dots, n-1\}$ and $i \in \{1, \dots, l\}$.

²Given $\mathbf{a}, \mathbf{b} \in F/R$, it can be effectively decided whether or not there exists an integer n such that $\mathbf{a} = \mathbf{b}^n$. Throughout this note we shall assume that F/R is recursively presented.

We write u as

$$u = \sum_{i=1}^l z_i \sigma_i,$$

where $z_i \in \mathbb{Z}A$. Then $(a-1)u = 0$ is equivalent to $(a-1)z_i = 0$ for each $i = 1, \dots, l$ and, in turn, $z_i = p(a)z_i^*$ for each $i = 1, \dots, l$. This gives $u = p(a)v$, where $v = \sum_{i=1}^l z_i^* \sigma_i$ is effectively determined.

The conjugacy in F/R' . In this section we shall prove the following result.

THEOREM. *If F/R has the solvable conjugacy problem and the solvable power problem, then F/R' has the solvable conjugacy problem.*

PROOF. Let F/R have the solvable conjugacy problem and the solvable power problem. Let T be a right transversal of F with respect to R . Let $\varphi(ra)$, $\varphi(sb)$ be given elements of F/R' where $r, s \in R$, $a, b \in T$. Then we wish to decide whether or not there is an element $\varphi(tc) \in F/R'$ with $t \in R$, $c \in T$ such that $\varphi(tc)\varphi(ra) = \varphi(sb)\varphi(tc)$. It is clearly necessary that $\mathbf{a}$ and $\mathbf{b}$ are conjugate in F/R . Thus we may assume that there exists $c \in T$ with $\mathbf{a} = \mathbf{c}^{-1}\mathbf{b}\mathbf{c}$. Since $\varphi^{-1}(c)\varphi(sb)\varphi(c) = \varphi(s'a)$ for some $s' \in R$ and since $\varphi(ra)$ and $\varphi(sb)$ are conjugate in F/R' if and only if $\varphi(ra)$ and $\varphi(s'a)$ are conjugate in F/R' , we may, without loss of generality, assume that the given elements are

$$\varphi(ra) = \begin{pmatrix} \mathbf{a} & \alpha(ra) \\ 0 & \mathbf{1} \end{pmatrix}$$

and

$$\varphi(sa) = \begin{pmatrix} \mathbf{a} & \alpha(sa) \\ 0 & \mathbf{1} \end{pmatrix}.$$

By Lemma 1, there exists

$$\begin{pmatrix} \mathbf{c} & f \\ 0 & \mathbf{1} \end{pmatrix} \in M$$

such that

$$\begin{pmatrix} \mathbf{c} & f \\ 0 & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{a} & \alpha(ra) \\ 0 & \mathbf{1} \end{pmatrix} = \begin{pmatrix} \mathbf{a} & \alpha(sa) \\ 0 & \mathbf{1} \end{pmatrix} \begin{pmatrix} \mathbf{c} & f \\ 0 & \mathbf{1} \end{pmatrix}$$

[if no such element of M exists then $\varphi(ra)$ and $\varphi(sa)$ are not conjugate in F/R']. Thus we have $c \in T$ and $f \in \Omega$ such that

$$(1) \quad \mathbf{c}\mathbf{a} = \mathbf{a}\mathbf{c}$$

and

$$(2) \quad (\mathbf{a} - \mathbf{1})f = \mathbf{c}\alpha(ra) - \alpha(sa)$$

if $a = 1$ we simply choose $c \in T$ such that $\mathbf{c}\alpha(r) = \alpha(s)$ (which is clearly decidable) and take $f = \alpha(c)$. If $a \neq 1$, then $\mathbf{c}\mathbf{a} = \mathbf{a}\mathbf{c}$ implies $ca = qac$ for some $q \in R$ and it follows that $\alpha(ca) = \alpha(qac)$, which gives (using Lemma 2)

$$(3) \quad (\mathbf{c} - \mathbf{1})\alpha(a) = (\mathbf{a} - \mathbf{1})\alpha(c) + \alpha(q)$$

Next,

$$\begin{aligned}
 c\alpha(ra) - \alpha(sa) &= c\{\alpha(a) + \alpha(r)\} - \{\alpha(a) + \alpha(s)\} \\
 &= (c-1)\alpha(a) + c\alpha(r) - \alpha(s) \\
 &= (a-1)\alpha(c) + \alpha(q) + c\alpha(r) - \alpha(s), \quad \text{by (3)} \\
 &= (a-1)\alpha(c) + \alpha(q(crc^{-1})s^{-1}), \quad \text{by Lemma 2.}
 \end{aligned}$$

Thus (2) gives

$$(4) \quad (a-1)f^* = \alpha(q^*)$$

where $f^* = f - \alpha(c)$ and $q^* = q(crc^{-1})s^{-1} \in R$. It remains to show that, in (4), f^* can be replaced by $\alpha(t)$ for some $t \in R$; for, then $(a-1)\alpha(t) = \alpha(q^*)$ implies

$$(a-1)\alpha(t) + (a-1)\alpha(c) = (a-1)\alpha(c) + \alpha(q^*)$$

and, in turn,

$$\begin{aligned}
 (a-1)\alpha(tc) &= (a-1)\alpha(c) + \alpha(q(crc^{-1})s^{-1}); \\
 (a-1)\alpha(tc) &= c\alpha(ra) - \alpha(sa);
 \end{aligned}$$

which implies that

$$\varphi(tc)\varphi(ra) = \varphi(sa)\varphi(tc).$$

Let $\alpha(q^*) = \sum_x g_x \lambda_x$ and $f^* = \sum_x f_x^* \lambda_x$. Then, as in [6], $(a-1)f^* = \alpha(q^*)$ gives, in turn,

$$\begin{aligned}
 (a-1)f_x^* &= g_x \quad \text{for all } x; \\
 (a-1)f_x^*(x-1) &= g_x(x-1) \quad \text{for all } x; \\
 (a-1) \sum_x f_x^*(x-1) &= \sum_x g_x(x-1) \\
 (a-1) \sum_x f_x^*(x-1) &= 0 \quad (\text{by Lemma 3, since } q^* \in R).
 \end{aligned}$$

If a is of infinite order in F/R , then $(a-1)u = 0$ in $Z(F/R)$ is possible only if $u = 0$. Thus $\sum_x f_x^*(x-1) = 0$ and, by Lemma 3, $f^* = \alpha(t)$ for some $t \in R$. If a is of finite order n , then by Lemma 4,

$$(5) \quad \sum_x f_x^*(x-1) = p(a)h$$

for some effectively determined $h \in Z(F/R)$ and $p(a) = 1 + a + \dots + a^{n-1}$. Since the left-hand side of (5) lies in the augmentation ideal of $Z(F/R)$, it follows that $h = \sum_x h_x(x-1)$, where h_x 's can be effectively determined (using $(gh-1) = g(h-1) + (g-1)$ and $(g^{-1}-1) = -g^{-1}(g-1)$ etc.). Then (5) gives

$$\sum_x (f_x^* - p(a)h_x)(x-1) = 0$$

and, by Lemma 3, there exists $t \in R$ such that

$$\sum_x (f_x^* - p(a)h_x)\lambda_x = \alpha(t).$$

Thus with $h^* = \sum_x h_x \lambda_x$,

$$f^* - p(a)h^* = \alpha(t)$$

and consequently,

$$(a-1)f^* = (a-1)\alpha(t)$$

as was to be proved.

COROLLARY. If F/F^n has the solvable conjugacy problem, then $F/[F^n, F^n]$ has the solvable conjugacy problem (F^n is the group generated by the n th powers of the elements of F).

REMARK. If F is finitely generated, then for $n = 2, 3, 4, 6$, F/F^n is finite (see, for instance, M. Hall [3, Chapter 18]) and so $F/[F^n, F^n]$ has the solvable conjugacy problem. If F is finitely generated then for n odd, $n \geq 665$, F/F^n has the solvable conjugacy problem (Adian [1, Theorem 3.5]) and so $F/[F^n, F^n]$ has the solvable conjugacy problem for all such n .

REFERENCES

1. S. I. Adian, *The Burnside problem and identities in groups*, Springer-Verlag, New York, 1979.
2. C. K. Gupta and N. D. Gupta, *Generalized Magnus embeddings and some applications*, Math. Z. **160** (1978), 75–87.
3. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.
4. W. Magnus, *On a theorem of Marshall Hall*, Ann. of Math. (2) **40** (1939), 764–768.
5. J. Matthews, *The conjugacy problem in wreath products and free metabelian groups*, Trans. Amer. Math. Soc. **121** (1966), 329–339.
6. V. N. Remeslennikov and V. G. Sokolov, *Some properties of a Magnus embedding*, Algebra and Logic **9** (1970), 342–349.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MANITOBA, WINNIPEG, MANITOBA
R3T 2N2, CANADA